REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-38 are pending in the application. The Examiner additionally stated that claims 1-38 are rejected. By this communication, claims 1, 10-13, 15, 23, 26-27, and 29-30 are amended. Hence, claims 1-38 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §112

The Examiner rejected claim 1 under 35 U.S.C. 112, second paragraph for failing to point out and distinctly claim the subject matter which Applicant regards as his invention, noting that claim 13 recites the limitation "said interrupting event" in claim 1, yet providing no antecedent basis therefor. The Examiner noted that the claim was interpreted to be dependent upon claim 6. Appropriate correction was required.

In response, Applicant amends claim 13 by this communication such that it depends from claim 6, thereby providing the required antecedent basis. Accordingly, it is requested that the rejection of claim 13 be withdrawn.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-5, 10-12, 14-23, 26-30, and 33-38 under 35 U.S.C. 103(a) as being unpatentable over Yup et al., US PGP No. 20020191784 (hereinafter, "Yup"). Applicant respectfully traverses the Examiner's rejections.

As per claims 1, 23, and 30, the Examiner noted that Yup discloses an apparatus for performing cryptographic operations, comprising:

- a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said one of the cryptographic operations comprises: *[see paragraphs 0038-0039]*
    - a plurality of CBC block cryptographic operations performed on a corresponding plurality of input text blocks; *[see paragraph 0040]*
- [CBC] mode logic, operatively coupled to said cryptographic instruction, configured to direct said computing device to update pointer registers and intermediate results for each of said plurality of [CBC] block cryptographic operations; and *[see paragraph 0025]*
- execution logic, operatively coupled to said [CBC] block pointer logic, configured to execute said one of the cryptographic operations. *[see paragraph [0041]*

The Examiner conceded that Yup is not explicit in teaching CBC block cryptographic operations, but that although Yup teaches cryptographic operations on multiple successive blocks of text, Yup does not expressly state that these cryptographic operations are of cipher block chaining mode. The Examiner further stated that as is evident in Applicant's disclosure, on paragraph 0012 of the specification, it is well known that all symmetric key algorithms employ the same types of modes, ECB, CBC, CFB, and OFB being examples that are disclosed and that, based on this, the Examiner deems it obvious for one of ordinary skill in the art to implement CBC or any other block cipher mode in conjunction with the system/apparatus taught by Yup.

Applicant respectfully disagrees with the Examiner's characterization and understanding of the prior art and the invention as recited in claims 1, 23, and 30 Thus, the following points are submitted in traversal of the rejection.

First, one skilled in the art will concur that a microprocessor includes an understood set of functions and logic elements. Generally speaking, a microprocessor is understood by those in the art to microprocessor be a programmable digital electronic component that incorporates the functions of a central processing unit (CPU) on a single integrated circuit (IC). The aforementioned aspects of the microprocessor according to the present

invention are very adequately disclosed within the instant application to include the ability to fetch and execute instructions that have been provided in an application program, to perform address translation, to load and store variables from/to memory, etc. As such, a microprocessor differs from a coprocessor, which is conventionally understood to supplement the functions of the CPU. Operations performed by the coprocessor may be floating point arithmetic, graphics, signal processing, string processing, or encryption, as has been discussed in the instant application. Coprocessors require the host main processor to fetch the coprocessor instructions and handle all other operations aside from the coprocessor functions. Accordingly, and as Applicant has discussed in the instant application, a microprocessor is not a coprocessor, nor is a coprocessor a microprocessor. Applicant has discussed the existence and disadvantages of present day cryptographic coprocessors, and has provided the present invention to overcome the disadvantages of such.

By this communication, Applicant amends claims 1, 23, and 30 to recite a microprocessor to more clearly identify the invention according to the present application. Consequently, the apparatus of Yup is not even a coprocessor. It is a circuit. Yup does not even mention or hint that his circuit may be construed as a coprocessor. Certainly, Yup does not disclose, suggest, allude to, or even hint that his circuit be construed or combined with other circuits to yield a coprocessor, much less a microprocessor.

For example, in claim 1, Applicant has specifically recited that a cryptographic instruction is *received by a microprocessor* as part of an instruction flow executing on said *microprocessor*. Such terminology is well understood and appreciated by one of ordinary skill in the art, and it is respectfully submitted that to equate a circuit as disclosed by Yup, or even a coprocessor, with a microprocessor is inconsistent with the terminology of the art. In summary, among other novel aspects and features, the technique according to the present invention provides a cryptographic instruction that a programmer can employ to directly program cryptographic operations into an application program, where such operations are performed by a microprocessor that provides a cryptography unit within its execution logic. This microprocessor is not a coprocessor, nor is it a simple circuit.

With the above summary in view, Applicant respectfully submits that claim 1 recites a cryptographic instruction is received by a microprocessor as part of an instruction flow executing on said microprocessor. Yup does not recite a cryptographic instruction. In contrast, Yup teaches a circuit being coupled to a system having a plurality of channels. The circuit 100 includes a plurality of input registers 102, one each coupled to the plurality of system channels. The input registers 102 are preferably simple first-in/first-out (FIFO) registers. The input registers 102 each receive a data string of a first predetermined bit length from its corresponding system channel. In the preferred embodiment, the predetermined bit length is 64 bits. The circuit 100 also includes a plurality of control signal input lines 103, one for each channel, coupled to receive control signals from systems and circuits external to the circuit 100. (Paragraphs 24-25)

Clearly, the circuit of Yup could be employed to perform AES encryption and decryption, but his circuit must be totally controlled via the input registers 102 and the control signal input lines 103. This is the way to perform these operations on the circuit of Yup.

In addition, claim 1 recites that OFB mode logic and an execution unit are coupled to the cryptographic instruction in the microprocessor. The OFB logic directs the microprocessor to update pointer registers and an initialization vector location for each of a plurality of OFB block cryptographic operations. The execution unit executes said one of the cryptographic operations. Yup does not teach these elements within a microprocessor because Yup does not teach or suggest a microprocessor at all, but rather a circuit that must be driven by control signal lines and provided with data over system channels.

Accordingly, it is respectfully requested that the rejection of claim 1 be withdrawn.

Independent claims 23 and 30 are amended to recite substantially similar limitations as are argued above as being allowable over Yup. Accordingly, it is requested that the rejections of claims 23 and 30 be withdrawn as well.

With respect to claims 2-5, 10-12, and 14-22, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup. Accordingly,

Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-5, 10-12, and 14-22.

With respect to claims 26-29, these claims depend from claim 23 and add further limitations that are neither anticipated nor made obvious by Yup. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 26-29.

With respect to claims 33-38, these claims depend from claim 30 and add further limitations that are neither anticipated nor made obvious by Yup. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 33-38.

The Examiner also rejected claims 6-9, 13, 24-25, and 31-32 under 35 U.S.C. 103(a) as being unpatentable over Yup in view of Sorimachi et al., US Patent No. 7184549, (hereinafter, "Sorimachi"). Applicant respectfully traverses the rejections and notes that claims 6-9 and 13 depend from claim 1, claims 24-25 depend from claim 23, and claims 31-32 depend from claim 30. All of these claims add further limitations over that subject matter which has been argued above as being allowable over the cited references. Accordingly, it is requested that the rejections of claims 6-9, 13, 24-25, and 31-32 be withdrawn.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-38 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

01/26/2008

Date: _____